



2250n Teaching and Learning Industrial **Control Systems Security Using Open Platform Infrastructure**

2025 CAE Symposium Charleston, SC April 8-10, 2025

mposium Dr. Guillermo Francia, III

In the beginning....Co

2009: NSF Major Research Infrastructure











2025 Portable RTUs

2011: Security of field devices









Training Tool Suite

2014: Faculty Development Workshop on ICS-SCADA Security







5

Contributions to the CAE Community



- An affordable infrastructure for an effective ICS security training;
- Useful insights into the design and implementation of ICS Open Platform Infrastructure (OPI);
- A method to validate of ICS vulnerability assessment and security testing tools; and
- A methodology to enable the introduction of upto-date, real-world ICS security scenarios to augment active learning.







Open Platform Infrastructure (OPI)

- Open Platform Infrastructure enables lightweight containers to securely run in isolation on a given host
- Containers can easily be shared and run on multiple hosts with the assurance that every host gets an identical container that works the same way (Docker (2024))



Ósiu

ICS-Open Platform Infrastructure (ICS-OPI) Design Guidelines



- Works on virtualized PLCs operating on standard ICS protocols;
- Occupies a small footprint and operates in isolation;
- Realizes an IT-OT network infrastructure;
- Facilitates the development of digital twins for ICS security;
- Enables interfacing with an external Human Machine Interface (HMI);
- Facilitates the simulation of ICS attacks and defenses by security purple teams.



This Photo by Unknown Author is licensed under <u>CC BY-SA-NC</u>





ICS-Open Platform Infrastructure (ICS-OPI) Design Implementations (cont)



Facilitates the development of digital twins for ICS security

-Combined OpenPLC, Docker containers, Network definitions on Dockercompose, and HMI implementation utilizing AdvancedHMI

Enables interfacing with an external Human Machine Interface (HMI)

-The implemented HMI is integrated with the softPLC



ICS-Open Platform Infrastructure (ICS-OPI) Design Implementations (cont)



- Reconnaissance
- Lateral movement
- Deep packet inspection
- ICS packet crafting
- Digital forensics
- Intrusion detection and prevention
- Threat intelligence and hunting

| | | . 7 8 6 9 9 3 3 5 8 8 2 2 9 4 5 5 9 3 3 3 4 1 | 82238374988285894212816579 |
|---|--|---|---|
| | *************************************** | 0141143118519637295109 | 397763555884886653162148686 |
| ********************************** | | 2 | 21704899029319610379514727 |
| *************************************** | | | 20441211723860868982991994 |
| | | 9241211574745251918288 | 17620924670056070869775274 |
| | | | 34484553858522527818483338 |
| | 44721483138883117928+8733364 | | 15476499628670814717863724 |
| ****717411688974668591621986 | 259943321967148476497550395 | 4 4 4 7 2 8 2 7 5 7 4 8 4 3 7 6 2 2 1 8 7 8 | 20871192114545124177542482 |
| *************************************** | 726226861467545588578662884 | | 55124738417066916888776458 |
| | 75654686162255786652885882481 | | 48536571358551884976921514 |
| 3 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 | 35863220108672719918861188 | | 11337089535448878315480813 |
| | 83692090341751684253553458 | 453561.891952581734737 | 54369349479575647272171373 |
| 2235845913112735378353681653 | 857862749674294849938887854 | 52656 | 1340720+325038821037340398 |
| 4 4 4 2 8 6 3 5 6 1 8 6 2 6 7 8 7 6 1 5 6 8 9 8 6 1 3 9 | 30247082659412847120554294 | | 1940384830396142835010 50 |
| 5521997396791027625016657496 | 21206600762341237588656065 | | 101831838916077374844 0 |
| 1487368927905469889144542922 | 4 4 7 5 8 2 9 7 64 4 6 7 8 3 44 8 8 8 8 3 5 6 | 4713112+1+1+47 | 5298434768462743741855 7 1 |
| 1774802422049470895034013952 | 3750.6240 30129 1 9739 4 | | 3 8 5 8 8 8 9 2 5 5 3 8 6 2 2 6 8 8 3 8 1 4 |
| 4414 .3528198532945474 | 506 562 25 54 863 655 . | · 2 9 4 3 9 9 9 05 1s e 2 | 998992626278693231835 |
| | *************************************** | 9 | 8936500115884378964752 15: |
| +++ d B 2 ++++++++++++++++++++++++++++++ | 3 4 4 + 4 2 7 4 3 4 7 9 4 3 4 7 4 1 4 1 7 + | | 313 623 41 1 7 63 62 6 9 6 3 4 6 3 80 782 |
| | 23 + 2 4 + 9 2 4 2 2 3 9 9 4 1 8 2 4 6 4 | 4 . 4 8 | *** 6 9 6 22 9* * * * 2 2 7 4 6 3 7 7 6 96 3 |
| EE+02 354 | 84 · · · · · · · · · · · · · · · · · · · | | . 57 6 308 2 30 2 8 4 1 6 3 4 4 9 8 67 80 |
| 2 2 4 M M M M M M M M M M M M M M M M M | 5 1 · · · · · · · · · · · · · · · · · · | | 1 1689 41741 4835385281 |
| 1 16 9 13232 | The survey of the local ball of the local states of the local stat | - S + + 1 # S + + 7 8 0 + | 1 1202+ 7 174 |
| 5 * ···· ····· 2 2 ····· 4 ·············· | 131 | 3 9 1 84 2 34 8 4 5 | 2 *** * * * * * * * * * * * * * * * * * |
| 17 6 19 | 11/ 12/ 12/ 12/54 | 3878699165474 | · · · 2 · · · 61 72 0 1 · · · · · · · · · · · · · · |
| 12 - 59 6 03 7 3111415445445245 | 1/1 / · · · · · · · · · · · · · · · · · | 1 1 6 - 652 147 017 89 5 3 | Free Sec. 2 - 43 8 31 11 3 31 48 |
| A set in the construction and a set and | | * 83 | 87. · · · · · · · · · · · · · · · · |
| AS ARRENT PROPERTY OF | A | 4 697120121327 | |
| | ************************************** | 0 · · · · · · · · · · · · · · · · · · · | TALE & BARRIER & BA |
| 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 | 8 | and the second second second | 3 |
| | 1 121117113471511117511114 | | ******** 0 3 01 7 7*** 4 ** 87 2* |
| 165 5 27 35 0 31 3 9148 | 2 2 2 4 1 1 1 1 1 1 6 1 1 + 3 1 2 4 1 4 | 147119 9660 | 8.7.5 ···· · · · · · · · · · · · · · · · · |
| 5 | 2 8 390 5 | 4 | 5 2 2 8 4 07 8 0 98 8** 1 6 *** 7 ** |
| 1 1 1 157 6 197 147 12 11 | 3 | 10 8 1 11 1 1 5 101 1 6 5 8 6 7 4 h 1 | 64 - 4 3 1 + 4 3 9 - 1 - 1 - 5 - 1 - 21 |
| 2 1 1 1 2 1 1 1 9 3 8 1 4 | 1// 1724118 113 12 12 12 14 14 14 14 14 14 14 14 14 14 14 | | 13737 |
| · · · · · · · · · · · · · · · · · · · | | 576435 516 211 | 4 7 61 2 842 99 93 1 2 1 37 18 15 |
| A 1994 A 1974 P 144 A 1974 | 37 * 5 4 2 123 139 1 2 5 2 3 3 1 2 1 5 4 7 7 | 55 1000 000784512 34514 | an ein gin ann ann ann ann ann ann a' Arr |
| agenticut d'entre la construction de | 1 - 50 7 1 + 1 + 1 21 - 62 51 7 - 1 20 + 82 - | 44 5 7 1 4 5 3 7 96 7 7 1 | 683 77 30 92 82 71 4 21 3 1 7 4 |
| ************************************** | 05 x 58 1 3 2 x 5 1 2 4 5 9 7 4 8 3 2 6 7 7 1 8 | 57 61823109 11 | 224 4 01 308 8 9 1 1 1 5 8 1 |
| ********* 6758 ****4 3 3 54 F* | 1 *9 2 * * *53 *53 * *97 1 * * * * * 9 * * * | 7 8 1 1 1 9 6 3 7 5 0 2 1 2 7 1 1 | 医白白白白 医外外的 医白白白 医黄金 医白白白白 医白白白 |
| CLERENCE CARD C | 4 * * 1 * * 3 6 1 7 1 4 * * 7 7 * 5 4 0 2 8 9 7 * * * * | 3095 241 41 7923111111 | ********* 03 233' + 35 5* 5 837+ |
| #\$ 19 2 46 49 38 43 2 1 19 7 4 2 4 8 4 2 5 8 1 7 | 1 **1 **3140702916918201*51*** | 11170579232042747160111 | 2 4 7 6 7 8 5 25 67 4 7 8 36 58 8 4 8 6 5 2 5 |
| 2 153761408 7920 11 14475 44756 | 9 45 723 9896144942 5 5 88598004 12 | 155' 47510" g* 871*2' ' ' ' | 3 14 3 24 7 1 7 9 1 1 5 2 9 8 2 1 5 2 4 7 |
| 9 38 761209 3 41033205 5 7 1 1 1 1 | and the state of t | | 41 29 8 29 1 29 1 4 1 |
| *************************************** | *************************************** | 1 | 22762394938351918732085703 |
| ************************* | ******************************* | | 16717669288222164862469419 |
| ******************************* | **************************** | *************************************** | 51279458621697491828437027 |
| | | *************************************** | 18170899923399827445588397 |
| THE REPORT OF THE PARTY OF THE | | | 19941719895456145455866058 |





Future Directions



- Expand the collection of ICS security case studies and scenarios to address newly discovered vulnerabilities
- Create virtual OPIs that incorporate devices found in renewable energy and power grid systems
- Expand and improve the creation of digital twins as instruments to carry out enhanced ICS security
- Automate the process of creating security scenarios for the effective utilization of digital twins in security training and education





Forthcoming ...



- Faculty development workshop at the UWF Center for Cybersecurity in Pensacola, FL. Travel stipend up to \$1200 afforded to faculty participants in July 2025.
- Complete OPI-ICS Security curriculum will be shared with the CAE community utilizing the CLARK System.







Acknowledgements

2025 C/ This work is partially supported by a subaward from the University of Memphis through a National Security Agency award under Federal Grant Number H98230-21-1-0319. The United States Government is authorized and distribute reprints notwithstanding any copyright







